Remarks

Claims 1-33, 56-82, and 91-104 are in the application. Claims 1, 17, 56, 65, and 91 are in independent form. Reconsideration is requested.

The amendment filed May 16, 2005 is objected to under 35 USC 132(a) as introducing new matter into the application. The Examiner states that the added material relates to authenticating for a first client a data object that is provided by a second client. Applicants respond as follows.

The abstract of the disclosure summarizes the invention as follows:

> A digital signature system is provided on a server for use by remote clients, such as by using a browser. The server generates and maintains all of the users' keys used for producing a digital signature. A user sends a data object to the server, and the server generates a digital signature for the data object using the private key stored at the server. The server then sends the digital signature to the client. A client can, at a later time, send the signature back to the server for verification.

Paragraph [0002] states that "the invention relates to a method, apparatus and product for providing digital signatures on electronic documents and for authenticating the documents by verifying their signatures." As further explained at paragraphs [0005] and [0006]:

> Electronic documents are replacing written contracts, orders, payment instruments, account statements, invoices, and other documents that have historically been signed by a written signature. It is frequently advantageous to have a document that has been produced and is being stored in digital form to have a digital signature applied to it so that the authentication of the signer can later be verified. The digitally-signed electronic document can then be transmitted for processing, without the need for a signed paper instrument.
>
> A need has arisen for alternative mechanisms for creating and authenticating legally binding electronic documents and communications. Digital encryption, digital message digests, digital signatures, and digital certificates are some of the existing cryptographic tools that are used in the present invention to address this need.

The background of the invention then describes the use of public key cryptography in digital authentication.

Applicants submit that digitally signing a document and later authenticating the signature inherently relates to a document that is signed by one party and authenticated

by another. There is no reasonable basis from the context of the present invention to consider a party applying a digital signature to an electronic document and later confirming the authenticity of the party's own signature. This inherent functionality is illustrated by the example of a purchase order being signed, as described in paragraphs [0079] and [0080] and referencing Appendices C and D, respectively. Purchase orders are passed from one party to another as part of a transaction. There is no circumstance that a purchase order signed by one party would later need to be authenticated by that party.

The use of one client to sign a document and another client to authenticate it is further illustrated at paragraph [0106], which states that:

> A Verification Receipt is a Verification Response that is signed at the server by the Requesting Party. A Verification Receipt allows the Requesting Party to prove to a third party, such as an original signer or an escrow agent, that the Requesting Party performed due diligence by verifying the signature at a specific point in time.

Applicants submit, therefore, that the May 16, 2005 amendment added no new matter to the present application. Applicants submit that the application clearly describes an invention that inherently relates to a first client signing an electronic document, and a second client later authenticating the signature of the first client. Applicants request, therefore, that the objection to the May 16, 2005 amendment be withdrawn.

Claims 1-33, 56-82, and 91-104 are rejected under 35 USC 112, second paragraph, as failing to comply with the written description requirement. The Examiner states that the added material relates to authenticating for a first client a data object that is provided by a second client. For the reasons set forth above in response to the objection to the May 16, 2005 amendment, applicants submit that the application claims include subject matter inherently included in the original application. Digitally signing a document and later authenticating the signature inherently relates to a document that is signed by one party and authenticated by another.

In particular, the application describes the invention in the context of providing digital signatures on electronic documents such as contracts, orders, payment

instruments, account statements, invoices, and other documents, and for authenticating the documents by verifying their signatures. This context inherently relates to documents signed by one party and authenticated by another. There is no reasonable basis from this context to consider a party applying a digital signature to an electronic document and later confirming the authenticity of the party's own signature. The application includes examples and illustrations that support the subject matter of the amended claims, as specified hereinabove.

Applicants submit, therefore, that the subject matter of the amended claims was included in the original application in such a way as to convey to one of skill in the art that the inventors were in possession of the claimed invention. Applicants request that this rejection be withdrawn.

Claims 17, 18, 56, 58, 59, 61, 62, 65, 67, 91 and 104 are rejected under 35 USC 112, second paragraph, for indefiniteness. The Examiner objects to the term "signing client." The claims have been amended to change the term "signing client" to "signature-requesting client" to clarify the claimed subject matter. (Applicants note that claim 91 does not include the rejected term.) Applicants request that the rejection be withdrawn.

Claims 91 and 104 are rejected under 35 USC 112, second paragraph, for indefiniteness. The Examiner objects to the term "verifying client." The claims have been amended to change the term "verifying client" to "signature-verifying client" to clarify the claimed subject matter. Applicants request that the rejection be withdrawn.

Claims 1-5, 8-19, 22-31, 33, 56-68, 70-80, 91-99, 102-104 are rejected under 35 USC 103(a) for obviousness over Vanstone (US Pat. No 6,490,682) in view of Pfitzmann. Claims 6 and 7 are rejected under 35 USC 103(a) for obviousness over Vanstone and Pfitzmann, and further in view of Pavlik (US Pat. No. 6,807,633). Claims 20, 21, 32, 69, 81, 82, and 100 are rejected under 35 USC 103(a) for obviousness over Vanstone and Pfitzmann, and further in view of Epstein (US Pat. No. 6,601,172). Applicants respond as follows.

Independent claims 1, 17, 56, 65, and 104 relate to an authenticating server, which in the language of claim 1 authenticates for a first client a data object that is provided by a second client. Applicants submit that independent claims 1, 17, 56, 65, and 104, and their respective dependent claims, are patentably distinct from the cited references for the following reasons.

As noted by the Examiner, Vanstone is directed to a log-on verification protocol that provides authentication in an information exchange between a client and a server. "This invention seeks to provides a solution to the problem of server verification by a client." (Vanstone, col. 1, lines 41-42.) The Examiner notes that Vanstone describes a client as verifying the validity of a signature, rather than the server, and cites Pfitzman as showing server-sided signing and verification.

Pfitzman describes general digital signature schemes, including a server-aided verification in which some verification computations are delegated to a server for clients with limited computational capabilities (e.g., smartcards). The Examiner adds that Pfitzmann also describes the use of Group-Oriented Signature Schemes "that allow for many users within a group to authenticate specific signers within their group using the server, which would meet the newly added limitations that amount to allowing a server to function as an authenticating intermediary."

Claim 1 recites an authentication method in which a data object from one client (a "second client") is authenticated for another client (a "first client") by method steps performed at a server. The method includes the steps of receiving the data object at the server from the second client to the server, generating at the server a signature corresponding to the second client, associating the signature with the data object at the server to create a signed object; delivering the signed object to the first client; and returning the signed object from the first client to the server to authenticate that the signature of the signed object corresponds to the second client. This method allows the

server to function as an authenticating intermediary for a data object passed between the first and second clients. Remaining independent claims 17, 56, 65, and 104 recite analogous subject matter.

Applicants submit that the direct log-on authentication of Vanstone, with server-side processing of Pfitzman, does not teach or suggest intermediary server authentication that allows an authenticated data object to be passed between two separate clients. In referencing the Group-Oriented Signature Schemes of Pfitzmann, the Examiner appears to acknowledge that the server-aided verification described on page 29 does not teach or suggest the intermediary server authentication recited in the claims. Applicants submit that even with the Group-Oriented Signature Schemes, the cited references do not teach or suggest the claimed subject matter.

Pfitzman describes general digital signature schemes, including a server-aided verification (page 29) in which some verification computations are delegated to a server for clients with limited computational capabilities (e.g., smartcards). This server-aided implementation is described in a sub-section entitled "Properties to Improve Efficiency." The title of the section that includes the sub-section has not been provided, but appears to be numbered as section 2.7.1.

The next section of Pfitzmann is directed to "Signature-Related Schemes," which includes a sub-section on Blind Signature Schemes, a sub-section on Group-Oriented Signature Schemes, and a sub-section on Identity-Based Signature Schemes. Pfitzmann describes the Group-Oriented Signature Schemes as follows:

> Sometimes people sign in the name of a group or an organization. It may then be useful that the group as such has a public key so that recipients need not know which individuals belong to the group. If the group members trust each other, they can simply generate one secret key and give it to each group member. Other schemes do not have specific group keys, they only let a number of people who all have their own key pairs sign a message such that the result is shorter than the list of individual signatures would be. (p. 30-31)

Pfitzmann is directed to summarizing separate digital signature features. As described above, one feature is server-aided verification in which some verification computations are delegated to a server for clients with limited computational capabilities (e.g., smartcards). The Examiner acknowledges that this feature does not teach or

suggest a server that functions as an authenticating intermediary, as recited in the claims.

Group-Oriented Signature Schemes are another digital signature feature described by Pfitzmann. Contrary to the Examiner's assertion, Pfitzmann provides no teaching or suggestion of using Group-Oriented Signature Schemes with the server-aided verification for devices having limited computational abilities. They are simply two different features in a book listing many different digital signature features. Applicants submit, therefore, that the rejection is improper and should be withdrawn because there is no teaching or suggestion to combine the server-aided verification with the unrelated Group-Oriented Signature Schemes of Pfitzmann.

Moreover, applicants submit that even if proper, the combination does not teach or suggest each and every element recited in the claims. As acknowledged by the Examiner, the server-aided verification of Pfitzmann does not teach or suggest a server that functions as an authenticating intermediary. However, the Group-Oriented Signature Schemes of Pfitzmann are directed primarily to each person in a group sharing a common public key. As an alternative, different people in a group may have their own public keys and may each sign a common document. The Group-Oriented Signature Schemes of Pfitzmann are directed only to group-use of a common public key or application of multiple public keys to a signature. The Group-Oriented Signature Schemes of Pfitzmann provide no teaching relating to using a server as an authenticating intermediary.

Neither Vanstone, nor Pfitzmann, nor any other cited reference, provides any teaching or suggestion of using a server as an authenticating intermediary. The cited references provide verification protocols that are operable only with direct communication. Pfitzmann then also describes that groups of people can share a common public key or may using multiple individual public keys to sign a document. Accordingly, applicants submit that the cited references do not teach or suggest the subject matter of any claims of the application. Applicants request, therefore that the rejections for obviousness be withdrawn.

Applicants believe the application is in condition for consideration and respectfully request the same.

IPSOLON LLP
805 SW BROADWAY #2740
PORTLAND, OREGON 97205
TEL. (503) 249-7066
FAX (503) 249-7068

Respectfully Submitted,

Mark M. Meininger
Registration No. 32,428